

Indépendance algébrique et exponentielle de Carlitz

par

LAURENT DENIS (Paris)

1. Position du problème. On désigne par $\mathbb{F}_q[T]$ l'anneau des polynômes en une variable à coefficients dans le corps fini \mathbb{F}_q de caractéristique p , par $k = \mathbb{F}_q(T)$ son corps des fractions, par $k_\infty = \mathbb{F}_q((1/T))$ le complété de k pour la valuation $(1/T)$ -adique v , que l'on prolonge à une clôture algébrique \bar{k} (resp. \bar{k}_∞) de k (resp. k_∞).

On notera $|\alpha| = q^{-v(\alpha)} = q^{\deg_T(\alpha)}$ la valeur absolue d'un élément de \bar{k}_∞ . Les éléments de \bar{k} seront parfois appelés *nombres algébriques*.

On désigne encore par t une indéterminée, par A l'anneau $\mathbb{F}_q[t]$ des polynômes en t et par $\deg_t a$ le degré d'un polynôme a de $\mathbb{F}_q[t]$, et on conviendra que $\deg_t 0 = -\infty$. Par t -module de dimension N , on entend la donnée d'un couple $E = ((G_a)^N, \Phi)$ où $(G_a)^N$ désigne le groupe additif de dimension N et Φ un homomorphisme injectif d'anneau de $\mathbb{F}_q[t]$ dans l'anneau $M_{N \times N}\{F\}$ des endomorphismes de $(G_a)^N$ vérifiant

$$\Phi(t) = a_0 F^0 + \dots + a_d F^d,$$

où les a_i ($0 \leq i \leq d$) sont des matrices $N \times N$ à coefficients dans \bar{k}_∞ avec $a_d \neq 0$, et F est l'endomorphisme de Frobenius sur $(G_a)^N$. Un *sous- t -module* H de E sera un sous-groupe algébrique connexe de $(G_a)^N$ vérifiant $\Phi(t)(H) = H$.

DÉFINITIONS. Pour tout entier $i \geq 1$, on pose $[i] = T^{q^i} - T$ et par récurrence $D_h = [h](D_{h-1})^q$ et $D_0 = 1$.

Le *module de Carlitz* est la donnée du groupe additif G_a et de l'homomorphisme d'anneau $\Phi_C : \mathbb{F}_q[T] \hookrightarrow \text{End}(G_a)$ défini par

$$\Phi_C(T) = TF^0 + F.$$

Il existe alors une unique fonction exponentielle $e(z)$, caractérisée par :

- 1) pour tout $z \in \bar{k}_\infty$, $(d/dz)(e(z)) = 1$;
- 2) pour tout $z \in \bar{k}_\infty$, $e(Tz) = Te(z) + e(z)^q$.

On déduit de ces propriétés l'expression (cf. [C])

$$e(z) = \sum_{h=0}^{\infty} \frac{z^{q^h}}{D_h}.$$

Rappelons aussi qu'il existe un élément $\pi \in k_{\infty}$ tel que $\text{Ker } e(z) = A(T - T^q)^{1/(q-1)}\pi$ (cf. [C]). On posera $\widehat{\pi} = (T - T^q)^{1/(q-1)}\pi$.

On note dorénavant par ' l'unique dérivation prolongeant continûment la dérivation d/dT de k à la clôture séparable $(k_{\infty})^s$ de k_{∞} . On notera encore k^s la clôture séparable de k .

On peut également définir la dérivée n -ième de l'exponentielle par rapport à T : elle est obtenue en dérivant terme à terme les coefficients de la série entière $e(z)$ (cf. [D3]). Pour $1 \leq n \leq p-1$, on trouve la dérivée d'ordre n non nulle :

$$e^{(n)}(z) = \sum_{h=1}^{\infty} \frac{(n!)z^{q^h}}{[h]^n D_h}.$$

Notons qu'on obtient $e^{(p)}(z) = 0$. On a vu dans [D3] :

THÉORÈME. *Soient $\alpha_1, \dots, \alpha_n \in \overline{k}_{\infty}$ linéairement indépendants sur k ; on a*

$$\deg_k \text{tr}(z, e(\alpha_1 z), \dots, e(\alpha_n z), \dots, e^{(p-1)}(\alpha_1 z), \dots, e^{(p-1)}(\alpha_n z)) = np + 1.$$

Sans dérivation cet énoncé a été prouvé par J. Yu [Y2]. Pour le cas général rappelons qu'on utilise dans [D3] le fait que ces fonctions sont toutes additives et donc, par un théorème d'Artin, que seuls des polynômes additifs peuvent donner des relations de dépendance algébrique entre ces fonctions. On conclut par une récurrence adéquate en utilisant les équations fonctionnelles satisfaites (rappelées au lemme 5 ci-dessous).

On peut alors formuler un analogue renforcé à la conjecture de Schanuel (voir par exemple [Wa]) :

CONJECTURE. *Soient $\alpha_1, \dots, \alpha_n$ appartenant à \overline{k}_{∞} et linéairement indépendants sur k ; alors*

$$\deg_k \text{tr}(\alpha_1, \dots, \alpha_n, e(\alpha_1), \dots, e(\alpha_n), \dots, e^{(p-1)}(\alpha_1), \dots, e^{(p-1)}(\alpha_n)) \geq np.$$

Comme dans le cas usuel, cette conjecture contient tous les résultats connus (voir [B-B-T], [Dj], $1 \leq j \leq 5$, [T2], [Yi], $1 \leq i \leq 5$) sur la transcendance des valeurs de la fonction exponentielle.

On se propose d'obtenir ici le résultat suivant :

THÉORÈME 1. *On suppose $p \geq 5$. Soient $\alpha, \beta \in \overline{k}_{\infty}$ linéairement indépendants sur k ; alors*

$$\deg_k \text{tr}(\alpha, \beta, e(\alpha), \dots, e^{(4)}(\alpha), e(\beta), \dots, e^{(4)}(\beta)) \geq 2.$$

De ce théorème on déduira le résultat suivant :

THÉOREME 2. *On suppose $p \geq 5$. Soient $\alpha, \beta \in (k_\infty)^s$ linéairement indépendants sur k ; alors*

$$\deg_k \operatorname{tr}(\alpha, \beta, e(\alpha), e'(\alpha), e(\beta), e'(\beta)) \geq 2.$$

Quand $p \geq 5$, ce résultat améliore le théorème 2 de [D3] où on obtenait le résultat :

THÉOREME. *Soient $\alpha, \beta, \gamma \in \bar{k}_\infty$ linéairement indépendants sur k ; alors*

$$\deg_k \operatorname{tr}(\alpha, \beta, \gamma, e(\alpha), e(\beta), e(\gamma), e'(\alpha), e'(\beta), e'(\gamma)) \geq 2.$$

Le théorème 2 permet ainsi d'améliorer les corollaires a), b), c) du théorème 1 de [D3] pour $p \geq 5$. On note $e = e(1)$. On rappelle à la demande du referee les corollaires au théorème 2 de [D3] :

COROLLAIRES. (a) *Pour $q \neq 2$, $\deg_k \operatorname{tr}(\pi, e, e(e), e', e'(e), e'(\widehat{\pi})) \geq 2$.*

(b) *$\deg_k \operatorname{tr}(\pi, e, e(\pi), e(\pi^2), e', e'(\pi), e'(\pi^2)) \geq 2$; et pour $q = 2$, $\deg_k \operatorname{tr}(\pi, e, e(\pi^2), e', e'(\pi), e'(\pi^2)) \geq 2$.*

(c) *$\deg_k \operatorname{tr}(e, e(e), e(e^2), e', e'(e), e'(e^2)) \geq 2$.*

On va ici prouver (au paragraphe 2) :

COROLLAIRE 1. *Pour $p \geq 5$:*

(a) *$\deg_k \operatorname{tr}(e, e(e), e', e'(e)) \geq 2$.*

(b) *Soient α, β des logarithmes de nombres algébriques séparables; alors $\deg_k \operatorname{tr}(\alpha, \beta, \alpha', \beta') \geq 2$.*

(Notons qu'on ne donne pas ici l'amélioration du (b), ce résultat étant dépassé par le corollaire (b) du théorème 3 ci-dessous.)

Remarque. Il est sans doute possible d'obtenir un énoncé semblable au théorème 1 valable pour tout p , en utilisant les dérivations divisées. Ce résultat demanderait toutefois un lemme de multiplicité concernant des T -modules plus généraux que ceux apparaissant dans le résultat de J. Yu [Y4] (et ceux de [A] et [A-T]). Cependant le défaut de composition de ces opérateurs ne semble pas alors permettre d'en déduire le théorème 2.

Une autre utilisation de la variable T pour obtenir des résultats d'indépendance algébrique est la méthode du changement de variable. Plus précisément, on va changer T en ξT où ξ est dans \mathbb{F}_q .

DÉFINITION. Soit ξ un élément de \mathbb{F}_q^* . On désigne par σ_ξ l'unique automorphisme continu de k_∞ tel que $\sigma_\xi(T) = \xi T$. On prolonge σ_ξ à $\bar{\mathbb{F}}_q((1/T))$ en décrétant que σ_ξ est l'identité sur $\bar{\mathbb{F}}_q$.

Cette méthode va conduire au résultat suivant :

THÉORÈME 3. *Soient donnés α et β , non nuls, dans k_∞ . On suppose qu'il existe $\xi \in \mathbb{F}_q^*$, a et $b \in \mathbb{Z}$ tels que $\sigma_\xi(\alpha) = \xi^a \alpha$ et $\sigma_\xi(\beta) = \xi^b \beta$.*

- (a) *Si $\xi \notin \{1, -1\}$, alors $e(\alpha)$ est transcendant sur $k(\beta)$.*
- (b) *Si $\xi \neq 1$ et si α est algébrique, alors $e(\alpha)$ est transcendant sur $k(\beta)$.*

En posant $e = e(1)$, on obtiendra également les corollaires suivants :

COROLLAIRE 2. (a) *Si $q \geq 3$, alors e et π sont algébriquement indépendants sur k .*

(b) *Si $q \geq 4$, et si $P \in \mathbb{F}_q[X]$ est non nul, alors $e(P(\pi))$ et π sont algébriquement indépendants sur k .*

(c) *Pour tout $\alpha \in \mathbb{F}_q((1/T^{q-1})) - \{0\}$ quand $q \geq 4$, $e(\alpha)$ est transcendant sur $k(\pi)$.*

Preuve. Voir paragraphe 5.

Au paragraphe 2 nous montrons que le théorème 1 entraîne le théorème 2 ainsi que les corollaires 1(a) et (b). On utilise pour cela la dérivation par rapport à T . La démonstration du théorème 1 suit de près celle du théorème 1 de [D3] et ne s'en écarte que par un ajout suffisant de fonctions qui n'est possible que pour $p \geq 5$. Au paragraphe 3 nous établissons les lemmes préliminaires qui seront utilisés au paragraphe 4 pour faire marcher la machine transcendante. A la fin de ce même paragraphe, on montre aussi comment on peut conserver une partie des résultats précédents (et plus spécialement le (b) du corollaire 1) quand $p = 3$. Enfin, le théorème 3 et ses corollaires sont démontrés au paragraphe 5.

2. Preuve du théorème 2. On rappelle que k^s désigne la clôture séparable de k dans \bar{k}_∞ et que $(k_\infty)^s$ est celle de k_∞ . Nous utiliserons la généralisation suivante du lemme 11 de [D3] (essentiellement aussi dans [Z-S]) :

LEMME 1. *Si α, β sont dans $(k_\infty)^s$ et que β est algébrique séparable sur $k^s(\alpha)$, alors β' est algébrique séparable sur $k^s(\alpha, \alpha')$.*

Preuve. Soit Q le polynôme minimal de β sur $k^s(\alpha)$. D'après l'hypothèse de séparabilité, $(\partial Q/\partial X)(\beta)$ n'est pas nul. La dérivation par rapport à T de la relation $Q(\beta) = 0$ entraîne

$$(\partial Q/\partial X)(\beta)\beta' + (\partial Q/\partial T)(\beta) = 0.$$

Or $\partial Q/\partial T$ est un polynôme à coefficients dans $k^s(\alpha, \alpha')$, donc β' est algébrique séparable sur $k^s(\alpha, \alpha')$.

Le cas des extensions inséparables va être traité à l'aide des lemmes suivants :

LEMME 2. Soient α, β dans $(k_\infty)^s$ tels que α soit algébrique inséparable sur $k(\beta)$ de degré d'inséparabilité p^r . Alors β' et toutes ses dérivées sont dans $k(\alpha^{p^r}, \beta)$.

Preuve. Les seules extensions algébriques de k incluses dans $(k_\infty)^s$ étant séparables (cf. lemme 11 de [D3]), α et β sont nécessairement transcendants. Il existe alors un plus petit entier $r \geq 1$ tel que α^{p^r} soit algébrique séparable sur $k(\beta)$ de degré d . Écrivons alors une relation, de degré en β minimal :

$$\sum_{i=0}^d \sum_{j,k} a_{ijk} T^j \beta^k \alpha^{ip^r} = 0, \quad a_{ijk} \in \mathbb{F}_q.$$

On dérive cette relation par rapport à T . Si β' est nul, il n'y a rien à montrer. Si le coefficient de β' est non nul, on en déduit le résultat du lemme 2. Dans le cas contraire, par minimalité, il faut que les dérivées de β^k soient nulles pour tout entier k . Donc seuls des multiples de p apparaissent dans les exposants de β . Parmi les relations du type précédent, on en choisit une de degré en T minimal, d'où l'on déduit de même que tous les exposants de T sont divisibles par p . La minimalité de r se trouve alors contredite.

LEMME 3. Soit $\alpha \in (k_\infty)^s$ tel que α' soit algébrique sur $k(\alpha)$; alors α' est algébrique séparable sur $k(\alpha)$.

Preuve. Si α est algébrique sur k , il n'y a rien à prouver. Si pour un $r \geq 1$, $(\alpha')^{p^r}$ est séparable sur $k(\alpha)$, alors d'après le lemme précédent, α' appartient à $k((\alpha')^{p^r}, \alpha)$ qui est une extension séparable de $k(\alpha)$.

LEMME 4. Soient α, β dans $(k_\infty)^s$ tels que α soit algébrique sur $k^s(\beta)$. Une condition nécessaire et suffisante pour que α soit séparable sur $k^s(\beta)$ est que $\alpha \in k^s(\alpha^p, \beta)$.

Preuve. On applique la proposition 4.9 de [L] à $K = k^s(\alpha, \beta)$, $k = k^s(\beta)$ et $m = 1$.

Preuve du théorème 2. Remarquons tout d'abord que si γ est dérivable, alors $(e(\gamma))' = e'(\gamma) + \gamma'$ et que pour $i \geq 1$, on a $(e^{(i)}(\gamma))' = e^{(i+1)}(\gamma)$. Le théorème de Wade ([W]) dit que si α est algébrique non nul, $e(\alpha)$ est transcendant; le degré de transcendance qu'on cherche à minorer est donc toujours ≥ 1 .

Supposons donc que

$$\deg_k \operatorname{tr}(\alpha, e(\alpha), e'(\alpha), \beta, e(\beta), e'(\beta)) = 1.$$

Si $e(\alpha) - \alpha$ est transcendant, alors l'hypothèse précédente entraîne que $e'(\alpha)$ est algébrique sur $k(e(\alpha) - \alpha)$. Comme $(e(\alpha) - \alpha)' = e'(\alpha)$, le lemme 3 montre que $e'(\alpha)$ est algébrique séparable sur $k(e(\alpha) - \alpha)$. Par des dérivations successives, on en déduit à l'aide du lemme 1 que $e^{(i)}(\alpha)$ est séparable sur $k(e(\alpha) - \alpha)$.

Si $e(\alpha) - \alpha$ est algébrique, sa dérivée $e'(\alpha)$ l'est également ainsi que toutes les dérivées d'ordre supérieur.

Dans les deux cas on obtient donc

$$\deg_k \operatorname{tr}(\alpha, e(\alpha), e'(\alpha), \dots, e^{(4)}(\alpha), \beta, e(\beta), e'(\beta)) = 1.$$

Le même raisonnement effectué avec β amène une contradiction avec le théorème 1.

Preuve du corollaire 1. (a) On applique le théorème 2 avec $\alpha = 1$ et $\beta = e$.

(b) On suppose $e(\alpha)$ et $e(\beta)$ algébriques séparables sur k . Toutes les extensions finies de k_∞ étant complètes, à l'aide du logarithme on montre aussi que α et β sont séparables sur k_∞ . Il reste alors à remarquer que les dérivées $e'(\alpha) + \alpha'$ et $e'(\beta) + \beta'$ sont également algébriques.

Remarque 1. Si α et β sont dans k_∞ et algébriquement dépendants sur k , on peut en fait montrer qu'au moins un des deux est séparable sur l'autre.

Remarque 2. On peut en particulier déduire du corollaire (b) qu'il existe des logarithmes de nombres algébriques α, β tels que α n'est pas algébrique séparable sur $k(\beta^p)$.

3. Lemmes préliminaires. Rappelons d'abord quelques propriétés des fonctions $e^{(n)}(z)$, $0 \leq n \leq p-1$ (cf. [D3], lemme 2).

LEMME 5. (1) *Pour tout $0 \leq n \leq p-1$, $e^{(n)}(z)$ est une E_q fonction au sens de J. Yu (cf. [Y1]), qui admet $((D_h)^{n+1})_{h \in \mathbb{N}}$ comme suite de dénominateurs.*

(2) $e(Tz) = Te(z) + e(z)^q$, $z + e'(Tz) = e(z) + Te'(z)$, et pour $2 \leq n \leq p-1$, $e^{(n)}(Tz) = ne^{(n-1)}(z) + Te^{(n)}(z)$.

On va utiliser le T -module Φ_4 (cf. [D3]), ce qui impose $p \geq 5$; c'est le T -module de dimension 6 déterminé par $\Phi_4(t) = A_0 F^0 + A_1 F^1$, où on a posé

$$A_0 = \begin{pmatrix} T & 0 & 0 & 0 & 0 & 0 \\ 0 & T & 0 & 0 & 0 & 0 \\ -1 & 1 & T & 0 & 0 & 0 \\ 0 & 0 & 2 & T & 0 & 0 \\ 0 & 0 & 0 & 3 & T & 0 \\ 0 & 0 & 0 & 0 & 4 & T \end{pmatrix}, \quad A_1 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

On a également vu dans [D3] (lemme 4) :

LEMME 6. *Les seuls sous- T -modules de $((G_a)^6, \Phi_4)$ sont $0, 0 \times 0 \times W$, où W est de la forme $W = 0^i \times (G_a)^{4-i}$ (pour un $0 \leq i < 4$), $0 \times (G_a)^5$, $G_a \times 0 \times (G_a)^4$ et $(G_a)^6$, chacun muni de la restriction naturelle de Φ_4 .*

Comme au lemme 5 de [D3], on montre

LEMME 7. $\Phi(z) = (z, e(z), e'(z), \dots, e^{(4)}(z))$ est un T -module à un paramètre de Φ_4 , c'est-à-dire, $\Phi(Tz) = \Phi_4(T)[\Phi(z)]$.

Nous allons maintenant utiliser le lemme de multiplicités de J. Yu. Soient $\alpha, \beta \in \bar{k}_\infty$ linéairement indépendants sur k ; on définit le sous-groupe suivant :

$$\Gamma(S) = \{\Phi(a\alpha + b\beta) : a, b \in A, \deg_T a, \deg_T b \leq S, S > 6\}.$$

LEMME 8. Soit P un polynôme non identiquement nul sur $(G_a)^6$ de multidegré $\leq (J, K, \dots, K)$. On suppose que P s'annule à un ordre $\geq 6M + 1$ aux points de $\Gamma(S)$, le long du T -module à un paramètre $\Phi(z)$. Il existe alors un réel $c > 0$ tel qu'au moins une des inégalités suivantes soit vérifiée :

$$Mq^{2S} \leq cJK^5 \quad \text{ou} \quad q^S \leq cK.$$

Preuve. Le lemme de zéros de J. Yu (Theorem 2.3 de [Y4]) donne l'existence d'un sous- T -module H de G , différent de G , et d'un réel $c > 0$ tels que

$$\binom{M + r(\Phi, H)}{r(\Phi, H)} \text{card}((\Gamma(S - 6) + H)/H) \mathbf{H}(H, J, K, \dots, K) \leq cJK^5,$$

où $r(\Phi, H)$ est la codimension analytique de $\Phi^{-1}(H)$ et \mathbf{H} désigne la fonction de Hilbert de H . L'examen des différents sous-groupes de G (voir lemme 6) va nous permettre d'aboutir à la conclusion du lemme.

Si $H = 0$, l'inégalité devient

$$Mq^{2S-6} \leq cJK^5;$$

si la projection de H sur la première coordonnée est 0, on a encore $r(\Phi, H) = 1$ et $\text{card}((\Gamma(S - 6) + H)/H) \geq q^{2S-6}$. Comme dans le lemme de zéros de [D3], les inégalités obtenues sont alors plus fortes que dans le cas $H = 0$.

Enfin, si $H = G_a \times 0 \times (G_a)^4$, on a $\Phi^{-1}(H) = \{a\hat{\pi} : a \in A\}$ et donc $r(\Phi, H) = 0$. Si $\Phi(z) \in H \cap \Gamma(S)$, alors $e(z) = 0$; le noyau de $e(z)$ étant de rang 1, $\text{card}(H \cap \Gamma(S)) \leq q^S$, d'où

$$q^{S-6} \leq cK.$$

En définitive, les deux conditions les moins contraignantes que l'on obtienne sont bien

$$Mq^{2S-6} \leq cJK^5 \quad \text{et} \quad q^{S-6} \leq cK.$$

Nous aurons également besoin d'un cas particulier du lemme de Siegel pour les extensions de type fini démontré par A. Thiery (proposition 4 de [T1]). On se donne θ_1, θ_2 dans \bar{k}_∞ tels que θ_1 soit transcendant sur k et θ_2 un entier algébrique séparable de degré D sur $A[\theta_1]$. On désigne alors

par s la taille sur $k(\theta_1, \theta_2)$ construite dans [T1]. Rappelons sa définition : si $x \in k(\theta_1, \theta_2)$, on peut écrire

$$x = \frac{\sum_{i=0}^{D-1} P_i(T, \theta_1) \theta_2^i}{P_D(T, \theta_1)},$$

et on pose $s(x) = \max \deg_{\text{total}}(P_i)$ et $N(x)$ désigne la norme de $k(\theta_1, \theta_2)$ sur $k(\theta_1)$. Il existe alors un réel $c_\theta > 0$ tel que :

- (s₁) pour tout $a, b \in A[\theta_1, \theta_2]$, $s(ab) \leq s(a) + s(b) + c_\theta$;
- (s₂) pour tout $a, b \in A[\theta_1, \theta_2]$, $s(a + b) \leq \max(s(a), s(b))$;
- (s₃) pour tout $x \in k(\theta_1, \theta_2)$, $s(N(x)) \leq c_\theta(1 + s(x))$;
- (s₄) pour tout $x \in k(\theta_1, \theta_2)$, $\deg_{\theta_1}(N(x)) \leq \deg_{\theta_1}(x) + c_\theta(1 + s(x))$.

On dispose alors du lemme suivant ([T1]) :

LEMME 9. Soient n, m des entiers naturels tels que $n > Dm$ et soient a_{ij} ($1 \leq i \leq n$, $1 \leq j \leq m$) des éléments de $A[\theta_1, \theta_2]$. Le système linéaire

$$\sum_{i=1}^n a_{ij} x_i = 0 \quad (1 \leq j \leq m)$$

admet une solution non triviale dans $A[\theta_1]$ avec

$$\max_{1 \leq i \leq n} s(x_i) \leq \frac{(Dm)^{1/2}}{n^{1/2} - (Dm)^{1/2}} \max s(a_{ij}) + 1.$$

Rappelons qu'on a posé pour tout $\alpha \in \bar{k}_\infty$, $|\alpha| = q^{\deg_T(\alpha)}$. On peut alors énoncer le lemme de Schwarz–Jensen (cf. J. Yu [Y1]).

LEMME 10. Soit $R > r > 0$ deux réels et f une fonction entière possédant ν_r zéros dans le disque $\deg_T(z) \leq r$; alors

$$M_r(f) \leq M_R(f) - \nu_r(R - r)$$

(où $M_r(f) = \sup_{\deg_T(z) \leq r} (\deg_T(f(z)))$).

Et enfin l'analogie du lemme de Gelfond obtenu par A. Thiery [T1] :

LEMME 11. Soit $\psi \in \bar{k}_\infty$ et $P_n \in A[X]$. On note

$$\delta_n = \deg_X(P_n), \quad h_n = h(P_n), \quad s_n = v(P_n(\psi))$$

et on suppose que pour tout $n \geq n_0$,

$$s_n > \max(h_n \delta_n + h_n \delta_{n+1} + h_{n+1} \delta_n, h_n \delta_n + h_n \delta_{n-1} + h_{n-1} \delta_n)$$

et

$$\lim_{n \rightarrow \infty} (s_n / \delta_n - h_n) = \infty.$$

Alors $P_n(\psi) = 0$ pour $n \geq n_0$.

4. La construction transcendant. On se place sous les hypothèses du théorème 1. D'après les résultats de Wade, si α est algébrique non nul, $e(\alpha)$ est transcendant. Pour prouver le théorème 1, on va donc supposer que le corps $L = k(\alpha, \beta, e(\alpha), e(\beta), \dots, e^{(4)}(\alpha), e^{(4)}(\beta))$ est de degré de transcendance 1 sur k et aboutir à une contradiction. On désigne par θ_1 une base de transcendance de L sur k et par L^s la sous-extension séparable maximale de $k(\theta_1)$ contenue dans L . D'après le théorème de Noether il existe alors θ_2 entier algébrique séparable sur $A[\theta_1]$ tel que $L^s = k(\theta_1, \theta_2)$. Il existe alors un entier naturel r tel que $\alpha^{p^r}, \beta^{p^r}, e(\alpha)^{p^r}, \dots, (e^{(4)}(\beta))^{p^r}$ appartiennent à L^s . D'après les équations fonctionnelles du lemme 5, il en est alors de même de $\alpha^{p^r}, e(a\alpha + b\beta)^{p^r}, (e'(a\alpha + b\beta))^{p^r}, \dots, (e^{(4)}(a\alpha + b\beta))^{p^r}$ pour tout $a, b \in A$. On désigne alors par $\Delta \in A[\theta_1, \theta_2]$ un dénominateur commun à $\alpha^{p^r}, \beta^{p^r}, e(\alpha)^{p^r}, \dots, (e^{(4)}(\beta))^{p^r}$.

LEMME 12. *Pour tout $a \in A$, Δ est un dénominateur de $(a\alpha)^{p^r}$ et de $(a\beta)^{p^r}$; $\Delta^{q^{\deg_T a}}$ est un dénominateur commun à $e(a\alpha)^{p^r}, \dots, (e^{(4)}(a\beta))^{p^r}$.*

Preuve. La première assertion est immédiate. Pour prouver la seconde, on s'aperçoit que $e(az) = \Phi_C(a)e(z)$ où $\Phi_C(a)$ est un élément unitaire de $A\{F\}$ de degré en F égal à $\deg_T a$. L'évaluation en α de cette égalité entraîne bien que $\Delta^{q^{\deg_T a}}$ est un dénominateur de $e(a\alpha)^{p^r}$ et de $e(a\beta)^{p^r}$. Par dérivation par rapport à T on a également $a'z + e'(az) = [\Phi_C(a)]'e(z) + ae'(z)$. Cette égalité avec $z = \alpha$ jointe aux propriétés précédentes montre que $\Delta^{q^{\deg_T a}}$ est un dénominateur de $(e'(a\alpha))^{p^r}$ et de $(e'(a\beta))^{p^r}$. La même méthode donne la conclusion pour les dérivées d'ordre supérieur.

On désignera par c_i ($1 \leq i \leq 14$) des réels strictement positifs qui ne dépendront que de α et de β . Construisons d'abord la fonction auxiliaire.

LEMME 13. *Il existe un polynôme P sur $(G_a)^6$ à coefficients dans $A[\theta_1]$ de multidegré $\leq (J, K, \dots, K)$ et non identiquement nul, tel que si*

$$DMq^{2S} < (J+1)(K+1)^5,$$

la fonction

$$F(z) = P(z^{p^r}, e(z)^{p^r}, \dots, (e^{(4)}(z))^{p^r})$$

s'annule à un ordre $\geq M$ aux points $a\alpha + b\beta$ avec $\max(\deg_T a, \deg_T b) \leq S$. De plus, il existe $c_1 > 0$ tel que

$$s(P) \leq c_1 \frac{(DMq^{2S})^{1/2}}{(JK^5)^{1/2} - (DMq^{2S})^{1/2}} (M \log_q M + SJ + q^S K) + 1.$$

Preuve. La première partie de ce lemme vient du lemme de Siegel avec $n = (J+1)(K+1)^5$, $m = Mq^{6S}$. Il reste à estimer la taille des coefficients du système linéaire pour conclure grâce au lemme 9. Ce système linéaire est obtenu en annulant les coefficients $\Delta_j(a, b)$ pour tout $a, b \in A$,

$\max(\deg_T a, \deg_T b) \leq S$ et $0 \leq j \leq M$ des expressions

$$P((\Phi(a\alpha + b\beta) + \Phi(z))^{p^r}) = \sum_{j \geq 0} \Delta_j(a, b) z^{q^j}.$$

Ces relations sont à coefficients dans $A[\theta_1, \theta_2]$ dès qu'on les a multipliées par le dénominateur $d_M = (D_h)^6 \Delta^J (\Delta^{q^{\deg_T a + \deg_T b}})^{5K}$ où l'entier h est le plus petit $\geq \log_q M + 1$ (cf. lemme 5). Il suffit donc, d'après les propriétés (s₁) et (s₂) de la taille (voir avant le lemme 9), de majorer la taille d'expressions de la forme

$$d_M (au_\varepsilon)^i e(au_\varepsilon)^{j_1} \dots (e^{(4)}(au_\varepsilon))^{j_5}$$

où $0 \leq i \leq J$, $0 \leq j_i \leq K$ et $\deg_T a \leq S$, $u_\varepsilon = \alpha$ ou β . On a

$$s(d_M) = 6 \deg_T D_h + Js(\Delta) + 5Kq^S s(\Delta) \leq M \log_q M + c_2(q^S K + J)$$

et $s(a^i) \leq SJ$, et on montre par récurrence sur S qu'il existe c_3 tel que

$$s(e^{(i)}(au_\varepsilon)) \leq c_3 q^S \quad (0 \leq i \leq 4),$$

d'où

$$s(d_M (au_\varepsilon)^i e(au_\varepsilon)^{j_1} \dots (e^{(4)}(au_\varepsilon))^{j_5}) \leq c_4 (M \log_q M + SJ + q^S K).$$

Ecrivons maintenant la suite des conditions à satisfaire pour obtenir le théorème 1. Considérons donc un polynôme P s'annulant sur $\Gamma(S)$. Il faut

$$Mq^{2S} \leq c_5 JK^5.$$

Cette condition est vérifiée en prenant $q^S = M^{96/100}$, $J = [M]$, $K = M^{42/100}$. Le lemme de Siegel montre alors

$$s(P) \leq c_1 \frac{(DMq^{2S})^{1/2}}{(JK^5)^{1/2} - (DMq^{2S})^{1/2}} (M \log_q M + SJ + q^S K) + 1.$$

Notons S' le plus grand entier tel que la fonction

$$F(z) = P(z^{p^r}, e(z)^{p^r}, \dots, (e^{(4)}(z))^{p^r})$$

s'annule à un ordre $\geq M$ aux points de $\Phi(a\alpha + b\beta)$ qui satisfont $\max(\deg_T a, \deg_T b) \leq S'$. On a bien sur $S' \geq S$. D'après le lemme de zéros on a également le renseignement

$$Mq^{2S'} \leq c_6 JK^5 \quad \text{ou} \quad q^{S'} \leq c_7 K.$$

Nous allons exclure la seconde alternative en imposant la condition

$$q^S > c_7 K,$$

qui est bien vérifiée au vu du choix des paramètres S et K .

Soient $R > r > S'$. Si on écrit $q^{S'} = M^{s'}$, on sait que (lemme de zéros et choix de S, J, K) $2s' \leq 210/100$, donc $s' < 105/100$. Il est donc possible de

prendre $q^r = M^{105/100}$ et $q^R = M^{110/100}$ pour que la condition $R > r > S'$ soit satisfaite. Le lemme 10 montre que pour tout $z \in \bar{k}_\infty$ de degré $< r$ on a

$$\deg_T(F(z)) \leq c_8(JR + Kq^R + s(P) - Mq^{2S'}(R - r)).$$

Comme on veut rendre ce terme petit, on regarde les conditions

$$Mq^{2S}(R - r) > JR + Kq^R + s(P).$$

Elles sont bien satisfaites pour $M > c_{11}$, grâce à nos choix de paramètres S, J, K, R, r .

Définissons $P_{a,b}(\theta_1) :=$ la norme sur $k(\theta_1)$ du M -ième coefficient du développement limité de P le long de Φ en $\Phi(a\alpha + b\beta)$ multiplié par le dénominateur $\Delta^J(\Delta^{q^{\deg_T a + \deg_T b}})^{5K}$ et estimons son degré en θ_1 . A l'aide de la propriété (s₄) du degré et de la taille, on obtient

$$\deg_{\theta_1}[P_{a,b}(\theta_1)] \leq c_9(JS' + Kq^{S'} + s(P)).$$

Enfin, la hauteur de $P_{a,b}$ est majorée par $s(P)$.

On utilise alors le lemme de Gelfond (lemme 11) et si la dernière condition suivante est remplie on a bien une contradiction :

$$Mq^{2S'}(R - r)[JS' + Kq^{S'} + s(P)]^{-1} > c_{10}s(P).$$

On vérifie encore que cette dernière est vérifiée avec les paramètres que l'on a choisi, pour $M > c_{12}$.

Regardons maintenant le cas $p = 3$. Il n'y a plus assez de fonctions dérivées pour obtenir tous les résultats précédents. En conservant les notations du paragraphe 4 et en supposant que $e(\alpha)$ et $e(\beta)$ sont algébriques, on s'aperçoit que le degré de $P_{a,b}$ est plus petit que précédemment. On va alors obtenir le résultat suivant :

THÉORÈME 1'. *On suppose $p \geq 3$. Soient $\alpha, \beta \in (k_\infty)^s$ linéairement indépendants sur k , tels que $e(\alpha)$ et $e(\beta)$ appartiennent à k^s . Alors*

$$\deg_k \operatorname{tr}(\alpha, \beta, e(\alpha), e'(\alpha), e^{(2)}(\alpha), e(\beta), e'(\beta), e^{(2)}(\beta)) \geq 2.$$

COROLLAIRE. *Sous les hypothèses du théorème 1',*

$$\deg_k \operatorname{tr}(\alpha, \beta, \alpha', \beta') \geq 2.$$

Le schéma de la preuve est identique à celui du paragraphe 4. On suppose donc que $\alpha, \beta, e(\alpha), e'(\alpha), e^{(2)}(\alpha), e(\beta), e'(\beta), e^{(2)}(\beta)$ sont dans une extension L algébrique inséparable sur $k(\theta_1, \theta_2)$. On va utiliser le lemme suivant :

LEMME 14. *Sous l'hypothèse que $e(\alpha), e(\beta) \in k^s$, il existe c_{13} tel que pour tout $a, b \in A$ on ait $\deg_{\theta_1}(e^{(i)}(a\alpha + b\beta)) \leq c_{13}$.*

Preuve. $e(a\alpha + b\beta)$ est algébrique, donc par dérivation $e^{(i)}(a\alpha + b\beta) + (a\alpha + b\beta)^{(i)}$ l'est également. Le degré en θ_1 d'un élément algébrique est nul. On conclut alors en prenant c_{12} plus grand que le degré de $\alpha, \alpha', \alpha'', \beta, \beta', \beta''$.

On reprend la preuve précédente. Définissons $P_{a,b}(\theta_1) :=$ la norme sur $k(\theta_1)$ du M -ième coefficient du développement limité de P le long de Φ en $\Phi(a\alpha + b\beta)$ multiplié par le dénominateur $\Delta^J(\Gamma^{q^{\deg_T a + \deg_T b}})^{5K}$ où Γ est cette fois dans A , et estimons son degré en θ_1 :

$$\deg_{\theta_1}[P_{a,b}(\theta_1)] \leq c_9(J + K + s(P)).$$

Ecrivons tous nos paramètres en fonction de M :

$$q^S = M^s, \quad q^{S'} = M^{s'}, \quad q^R = M^R, \quad q^r = M^r, \quad J = M^j, \quad K = M^k.$$

En reprenant alors la même preuve que ci-dessus mais avec le nouveau contrôle de $\deg_{\theta_1}[P_{a,b}(\theta_1)]$, pour $M > c_{14}$, on voit que toutes les inégalités nécessaires sont satisfaites avec les choix $j = 1$, $s = 60/100$, $k = 42/100$. On trouve $s' < 64/100$, on choisit alors $r = 64/100$ et $R = 65/100$.

5. La méthode du changement de variable. On conserve les notations du paragraphe 1 et la définition de σ_ξ de ce même paragraphe ($\sigma_\xi(T) = \xi T$). On montre d'abord quelques lemmes préliminaires.

LEMME 15. $\sigma_\xi(D_h) = \xi^h D_h$.

Preuve. Par récurrence sur h .

DÉFINITION. On pose

$$e_\xi(z) = \sum_{h=0}^{\infty} \frac{\xi^{-h} z^{q^h}}{D_h}.$$

Donnons quelques propriétés de ces fonctions :

LEMME 16. (i) Soit μ une solution de l'équation $X^{q-1} = 1/\xi$. Alors $\mu \in \overline{\mathbb{F}_q} - \mathbb{F}_q$ et pour tout $z \in \overline{k}_\infty$, $e_\xi(z) = e(\mu z)/\mu$.

(ii) $e_\xi(z)$ est la fonction exponentielle du T -module Φ_ξ de rang 1 défini par $\Phi_\xi(T) = TF + \xi^{-1}F$.

(iii) $\sigma_\xi(e(z)) = e_\xi(\sigma_\xi(z))$.

Preuve. (i) μ n'est pas dans \mathbb{F}_q car ξ est différent de 1. On prouve par récurrence sur h que $\mu^{q^h-1} = \xi^{-h}$, ce qui entraîne bien $e_\xi(z) = e(\mu z)/\mu$.

(ii) On vérifie l'équation fonctionnelle $e_\xi(Tz) = Te_\xi(z) + \xi^{-1}e_\xi(z)^q$.

(iii) Suit du lemme 15.

On va maintenant utiliser des analogues aux résultats de Lindemann–Weierstraß et de Gelfond–Schneider démontrés respectivement par Thiery et par Becker, Brownawell et Tubbs. Pour le module de Carlitz le résultat de [T2] s'énonce de la manière suivante :

THÉORÈME [T2]. Soient $\alpha_1, \dots, \alpha_n \in \overline{k}$, linéairement indépendants sur k . Alors $e(\alpha_1), \dots, e(\alpha_n)$ sont algébriquement indépendants sur k .

Dans le cadre du module de Carlitz le corollaire 1 de [B-B-T] est le suivant :

THÉOREME [B-B-T]. *Soit $\gamma \in \bar{k}$, de degré $c \geq 3$ sur k , et $u \in \bar{k}_\infty^*$, tel que $k(\gamma) \cap 1/u(\Lambda) = \{0\}$; alors*

$$\deg_k \operatorname{tr}(e(u), e(u\gamma), \dots, e(u\gamma^{c-1})) \geq 2.$$

On peut alors prouver le théorème 3 :

Preuve du théorème 3. Soient $\alpha, \beta \in k_\infty$ différents de zéro tels que $\sigma_\xi(\alpha) = \xi^a \alpha$ et $\sigma_\xi(\beta) = \xi^b \beta$. Supposons que $e(\alpha)$ soit algébrique sur $k(\beta)$. En appliquant σ_ξ à une relation de dépendance algébrique, il vient que $\sigma_\xi(e(\alpha))$ est algébrique sur $k(\sigma_\xi(\beta))$. Le (iii) du lemme 16 et la \mathbb{F}_q -linéarité de $e(z)$ montrent que ceci est équivalent au fait que $e_\xi(\alpha)$ est algébrique sur $k(\beta)$.

Or d'après le (i) du lemme 16, $e_\xi(\alpha) = e(\mu\alpha)/\mu$. De proche en proche, il s'ensuit que $e(\mu\alpha), e(\mu^2\alpha), \dots, e(\mu^{c-1}\alpha)$, où $c = \deg(u)$, sont aussi algébriques sur $k(\beta)$. Pour prouver le (a) du théorème, on applique le théorème de [B-B-T] ci-dessus avec $\gamma = \mu$ et $\alpha = u$. L'hypothèse sur α est bien vérifiée car un élément non nul du réseau des périodes Λ n'est pas dans $\bar{\mathbb{F}}_q((1/T))$ car $q \neq 2$ (voir la description du réseau au paragraphe 1). Prouvons que μ est de degré ≥ 3 . Il faut montrer que μ n'est pas dans une extension de degré 2 de \mathbb{F}_q , ce qui équivaut à $\mu^{q^2} = \mu$. Comme $\mu^{q^2-1} = 1/\xi^2$, il suffit que ξ soit différent de 0, 1, -1.

Pour prouver le (b), on remarque que comme $\xi \neq 0, 1$, μ n'est pas dans \mathbb{F}_q , et le raisonnement précédent montre que si la conclusion du théorème est fautive, alors $e(\alpha)$ et $e(\mu\alpha)$ sont algébriquement dépendants. On a alors une contradiction avec le théorème de [T2].

On prouve maintenant le corollaire 2.

Preuve du corollaire. (a) On dispose de l'expression suivante :

$$\pi = \prod_{i=0}^{\infty} \left(1 - \frac{[i]}{[i+1]} \right).$$

Comme $[i] = T^{q^i} - T$, ce nombre est donc invariant par tous les σ_ξ , il suffit alors d'appliquer le cas (b) du théorème 3 à $\alpha = 1$, $\beta = \pi$, et $a = b = 0$.

(b) On applique le cas (a) du théorème à $\alpha = \beta = P(\pi)$.

(c) α est invariant par tous les σ_ξ . En prenant $\beta = \pi$, le théorème 3 montre que $e(\alpha)$ est transcendant sur $k(\pi)$.

En liaison avec les dérivées qui apparaissent aux paragraphes précédents, on a aussi :

COROLLAIRE 3. *Si $q \geq 3$ et $0 \leq m \leq p-1$, alors e et $\pi^{(m)}$ sont algébriquement indépendants sur k .*

Preuve. Comme $\sigma_\xi(\pi) = \pi$, par dérivation on a $\sigma_\xi(\pi^{(m)}) = \xi^{-m}\pi^{(m)}$. On sait également que $\pi^{(m)}$ est transcendant ([D4]). Il reste alors à appliquer le théorème 3 avec $\alpha = 1$, $\beta = \pi^{(m)}$, $a = 0$, $b = -m$.

Terminons en signalant une conjecture liée à la méthode de changement de variable mais qui ne semble pas se déduire de notre conjecture de Schanuel généralisée :

CONJECTURE. *Soit λ un entier naturel strictement plus grand que 1. Alors pour tout $\alpha \in \mathbb{F}_q((1/T^\lambda)) - \{0\}$, $e(\alpha)$ est transcendant.*

PROPOSITION. *Le résultat de cette conjecture est vrai dans les cas suivants : (a) $q > 3$ et $\lambda = q - 1$, (b) $\lambda = p$.*

Preuve. Le cas (a) vient du corollaire (c) du théorème 3. Le cas (b) vient du théorème 3 de [D4] où l'on montre en particulier que la dérivée d'un logarithme de nombre algébrique est non nulle.

Références

- [A] G. Anderson, *t-motives*, Duke Math. J. 53 (1986), 457–502.
- [A-T] G. Anderson and D. Thakur, *Tensor powers of the Carlitz module and zeta values*, Ann. of Math. 132 (1990), 159–191.
- [B-B-T] P.-G. Becker, W. D. Brownawell and R. Tubbs, *Gelfond's theorem for Drinfeld modules*, Michigan Math. J. 41 (1994), 219–233, and Abstracts Amer. Math. Soc. 82 (1992), 359.
- [C] L. Carlitz, *On certain functions connected with polynomials in a Galois field*, Duke Math. J. 1 (1935), 137–168.
- [D1] L. Denis, *Théorème de Baker et modules de Drinfeld*, J. Number Theory 43 (1993), 203–215.
- [D2] —, *Remarques sur la transcendance en caractéristique finie*, C. R. Acad. Sci. Canada 14 (1992), 157–162.
- [D3] —, *Transcendance et dérivées de l'exponentielle de Carlitz*, dans: Séminaire de Théorie des Nombres de Paris, Birkhäuser, 1993, 1–21.
- [D4] —, *Dérivées d'un module de Drinfeld et transcendance*, soumis pour publication.
- [D5] —, *Indépendance algébrique sur le module de Carlitz*, C. R. Acad. Sci. Paris Sér. I 317 (1993), 913–915.
- [L] S. Lang, *Algebra*, 3rd ed., Addison-Wesley, 1993.
- [T1] A. Thiery, *Indépendance algébrique de périodes et quasi-périodes de modules de Drinfeld*, dans: The Arithmetic of Function Fields, Proceedings of the Workshop at Ohio State University, D. Goss, D. Hayes, M. Rosen (eds.), Walter de Gruyter, 1992, 265–284.
- [T2] —, *Théorème de Lindemann–Weierstrass pour les modules de Drinfeld*, Thèse de l'Université de Caen, et preprint, 1992.
- [W] L. Wade, *Transcendance properties of the Carlitz Ψ function*, Duke Math. J. 13 (1946), 79–85.
- [Wa] M. Waldschmidt, *Nombres transcendants*, Lecture Notes in Math. 402, Springer, 1974.

- [Y1] J. Yu, *Transcendence theory over function fields*, Duke Math. J. 52 (1985), 517–527.
- [Y2] —, *Transcendence and Drinfeld modules: Several variables*, *ibid.* 58 (1989), 559–575.
- [Y3] —, *Transcendence and special zeta values in characteristic p* , Ann. of Math. 134 (1991), 1–23.
- [Y4] —, *Analytic homomorphisms into Drinfeld modules*, preprint, 1991.
- [Y5] —, *A six exponentials theorem in finite characteristic*, Math. Ann. 272 (1985), 91–98.
- [Z-S] O. Zariski and P. Samuel, *Commutative Algebra*, Vol. 1, Springer, 1979.

UNIVERSITÉ PIERRE ET MARIE CURIE
U.F.R. 920 “PROBLÈMES DIOPHANTIENS”
4, PLACE JUSSIEU
TOUR 45-46, 5IÈME ÉTAGE
75252 PARIS, FRANCE

Reçu le 25.10.1993
et révisé le 1.3.1994

(2511)